Foundation of Cryptography, Lecture 8
Encryption Schemes

Handout Mode

Iftach Haitner, Tel Aviv University

Tel Aviv University.

April 29, 2014

Section 1

Definitions

Correctness

Definition 1 (encryption scheme)

A trippet of PPTM's $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ such that

1. $\mathsf{G}(1^n)$ outputs $(e, d) \in \{0,1\}^* \times \{0,1\}^*$
2. $\mathsf{E}(e, m)$ outputs $c \in \{0,1\}^*$
3. $\mathsf{D}(d, c)$ outputs $m \in \{0,1\}^*$

Correctness: $\mathsf{D}(d, \mathsf{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(\mathsf{G}(1^n))$ and $m \in \{0,1\}^*$

- e – encryption key, d – decryption key
- m – plaintext, $c = \mathsf{E}(e, m)$ – ciphertext
- $E_e(m) \equiv E(e, m)$ and $D_d(c) \equiv D(d, c)$,
- public/private key

Security

- What would we like to achieve?
- Attempt: for any $m \in \{0,1\}^*$:

$$(m, E_{(G(1^n))_1}(m)) \equiv (m, U_{\ell(|m|)})$$

  - Shannon – only possible in case $|m| \leq |G(1^n)_1|$
  - Other concerns: multiple encryptions, active adversaries, ...

Semantic Security

1. Ciphertext reveals no "computation information" about the plaintext
2. Formulate via the *simulation paradigm*
3. Does not hide the message *length*

Definition 2 (Semantic Security — private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if $\forall$ PPTM A, $\exists$ PPTM A' s.t. :
$\forall$ poly-length dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and poly-length functions $h, f\colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big| \Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m\leftarrow\mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Big| = \operatorname{neg}(n)$$

- Non uniformity is inherent.
- Public-key variant — A and A' get e
- Reflection to $\mathcal{ZK}$
- We sometimes omit 1^n and $1^{|m|}$

Indistinguishablity of Encryptions

- The encryption of two strings is indistinguishable
- Less intuitive than semantic security, but easier to work with

Definition 3 (Indistinguishablity of encryptions — private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions in the private-key model, if for any $p, \ell \in \text{poly}$, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n \in \mathbb{N}}$

$$\{(z_n, E_e(x_n))_{e \leftarrow G(1^n)_1}\}_{n \in \mathbb{N}} \approx_c \{(z_n, E_e(y_n))_{e \leftarrow G(1^n)_1}\}_{n \in \mathbb{N}}$$

- Non uniformity is inherent.
- Public-key variant — the ensemble contains e

Equivalence of Definitions

Theorem 4

An encryption scheme (G, E, D) *is semantically secure iff is has indistinguishable encryptions.*

We prove the private key case

Indistinguishability $\Longrightarrow$ Semantic Security

Fix $\mathcal{M}$, A, f and h, as in Definition 2.

Algorithm 5 (A′)

Input: 1^n, $1^{|m|}$ and $h(m)$

1. $e \leftarrow G(1^n)_1$
2. $c = E_e(1^{|m|})$
3. Output $\mathsf{A}(1^n, 1^{|m|}, h(m), c)$

Claim 6

A′ is a good simulator for A (according to Definition 2)

Proof: Let

$$\delta(n) := \Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(h(m), E_e(m)) = f(m)] - \Pr_{m \leftarrow \mathcal{M}_n}[\mathsf{A}'(h(m)) = f(m)]$$

We define an algorithm that distinguish two between two ensembles $\{x_n\}_{n\in\mathbb{N}}$ and $\{y_n\}_{n\in\mathbb{N}}$, with advantage $\delta(n)$.

Hence, the indistinguishability of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ yields that $\delta(n) \leq \mathrm{neg}(n)$.

The Distinguisher

Claim 7

For every $n \in \mathbb{N}$, exists $x_n \in \mathrm{Supp}(\mathcal{M}_n)$ with
$\Pr_{e \leftarrow G(1^n)_1}[\mathsf{A}(h(x_n), E_e(x_n)) = f(x_n)] - \Pr[\mathsf{A}'(h(x_n)) = f(x_n)] \geq \delta(n)$.

Proof: ?

Algorithm 8 (B)

Input: $1^n, 1^t, h', f', c$
Output 1 iff $\mathsf{A}(1^n, 1^t, h', c) = f'$

Let $\{z_n = (1^n, 1^{|x_n|}, h(x_n), f(x_n))\}_{n \in \mathbb{N}}$.

- $\Pr_{e \leftarrow G(1^n)}[\mathsf{B}(z_n, E_e(x_n)) = 1] =$
  $\Pr_{e \leftarrow G(1^n)_1}\left[\mathsf{A}(1^n, 1^{|x_n|}, h(x_n), E_e(x_n)) = f(x_n)\right]$
- $\Pr_{e \leftarrow G(1^n)}\left[\mathsf{B}(z_n, E_e(1^{|x_n|})) = 1\right] = \Pr\left[\mathsf{A}'(1^n, 1^{|x_n|}, h(x_n)) = f(x_n)\right]$

Hence,

$$\Pr_{e \leftarrow G(1^n)}[\mathsf{B}(z_n, E_e(x_n)) = 1] - \Pr_{e \leftarrow G(1^n)}\left[\mathsf{B}(z_n, E_e(1^{|x_n|})) = 1\right] \geq \delta(n),$$

Semantic Security $\implies$ Indistinguishability

For PPT B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n\}_{n\in\mathbb{N}}$, let

$$\delta(n) = \Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(y_n)) = 1]$$

We define distribution $\mathcal{M}$, functions f, h and algorithm A that has no $\delta(n)/4$ simulator. The semantic security of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ yields that $\delta(n) \leq \operatorname{neg}(n)$.

Let $f(x_n) = 1$ and $f(y_n) = 0$, and let $\mathsf{A}(w)$ output 1 if $\mathsf{B}(w) = 1$, and a uniform bit otherwise.

Claim 9

$\Pr_{e\leftarrow G(1^n)_1, t_n\leftarrow\{x_n,y_n\}}[\mathsf{A}(z_n, E_e(t_n)) = f(t_n)] = \frac{1}{2} + \frac{\delta(n)}{4}$

Proof: Let $\alpha(n) = \Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(x_n)) = 1]$.

$$\Pr_{e\leftarrow G(1^n)_1}[\mathsf{A}(z_n, E_e(x_n)) = f(x_n)] = \alpha(n) + \frac{1}{2}(1-\alpha(n)) = \frac{1}{2} + \frac{\alpha(n)}{2}$$

and

$$\Pr_{e\leftarrow G(1^n)_1}[\mathsf{A}(z_n, E_e(y_n)) = f(y_n)] = \frac{1}{2} + \frac{\delta(n)-\alpha(n)}{2}$$

Semantic Security $\implies$ Indistinguishability, cont.

- Let $\mathcal{M}_n$ be x_n w.p. $\frac{1}{2}$, and y_n otherwise.
- Let $h(1^n, \cdot) = z_n$, and recall $f(x_n) = 1$ and $f(y_n) = 0$.

By Claim 9:

$$\Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1} [\mathsf{A}(h(1^n, m), E_e(m)) = f(m)] = \frac{1}{2} + \frac{\delta(n)}{2}$$

But, for any A':

$$\Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1} [\mathsf{A}'(h(1^n, m)) = f(m)] \leq \frac{1}{2}$$

Hence, $\delta(n) \leq \text{neg}(n)$.

Security Under Multiple Encryptions

Definition 10 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any $p, \ell, t \in \mathrm{poly}$, $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$, PPTM B:

$$\Big| \Pr_{e \leftarrow G(1^n)_1} \left[\mathsf{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1\right] - \Pr_{e \leftarrow G(1^n)_1} \left[\mathsf{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1\right] \Big| = \mathrm{neg}(n)$$

Extensions:

- Different length messages
- Semantic security version
- Public-key variant

Multiple Encryption in the Public-Key Model

Theorem 11

A public-key encryption scheme has indistinguishable encryptions for multiple messages, iff it has indistinguishable encryptions for a single message.

Proof: Let $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ be a public-key encryption scheme that has no indistinguishable encryptions for multiple messages, with respect to PPT B, $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$.

Hence, for some function $i(n) \in [t(n)]$:

$$\Big| \Pr_{e\leftarrow \mathsf{G}(1^n)_1}\left[\mathsf{B}(1^n, e, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), E_e(y_{n,i}) \ldots, E_e(y_{n,t(n)})) = 1\right]$$
$$- \Pr_{e\leftarrow \mathsf{G}(1^n)_1}\left[\mathsf{B}(1^n, e, E_e(x_{n,1}), \ldots, E_e(x_{n,i}), E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)})) = 1\right] \Big|$$
$$> \operatorname{neg}(n).$$

Thus, $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has no indistinguishable encryptions for single message:

Algorithm 12 (B')

Input: 1^n, $z_n = (i(n), x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)})$, e ,c
Return $\mathsf{B}(c, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), c, E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)}))$

Multiple Encryption in the Private-Key Model

Fact 13

Assuming (non uniform) OWFs exists, then $\exists$ encryption scheme that has private-key indistinguishable encryptions for a single messages, but not for multiple messages.

Proof: Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{n+1}$ be a (non-uniform) PRG, and for $i \in \mathbb{N}$ let g^i be its "iterated extension" to output of length $n+i$ (see Lecture 2).

Construction 14

- $\mathsf{G}(1^n)$: outputs $e \leftarrow \{0,1\}^n$
- $\mathsf{E}_e(m)$: outputs $g^{|m|}(e) \oplus m$
- $\mathsf{D}_e(c)$: outputs $g^{|c|}(e) \oplus c$

Multiple Encryption in the Private-Key Model, cont.

Claim 15

(G, E, D) has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it:

$$\left|\Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus x_n) = 1] - \Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus y_n) = 1]\right| > \operatorname{neg}(n) \quad (1)$$

Hence, B yields a (non-uniform) distinguisher for g. (?)

Claim 16

(G, E, D) does not have a private-key indistinguishable encryptions for multiple messages

Proof: Take $x_{n,1} = x_{n,2}$ and $y_{n,1} \neq y_{n,2}$, and let B be the algorithm that on input (c_1, c_2), outputs 1 iff $c_1 = c_2$.$\square$

Section 2

Constructions

Private-Key Indistinguishable Encryptions for Multiple Messages

Suffices to encrypt messages of some fixed length (here the length is n).(?)

Let $\mathcal{F}$ be a (non-uniform) length-preserving PRF

Construction 17

- $\mathsf{G}(1^n)$: output $e \leftarrow \mathcal{F}_n$
- $\mathsf{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(r, e(r) \oplus m)$
- $\mathsf{D}_e(r, c)$: output $e(r) \oplus c$

Claim 18

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has private-key indistinguishable encryptions for a multiple messages

Proof: ?

Public-key indistinguishable encryptions for multiple messages

Let (G_T, f, Inv) be a (non-uniform) TDP, and let b be hardcore predicate for it.

Construction 19 (bit encryption)

- $\mathrm{G}(1^n)$: output $(e, d) \leftarrow \mathrm{G}_T(1^n)$
- $\mathrm{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(y = f_e(r), c = b(r) \oplus m)$
- $\mathrm{D}_d(y, c)$: output $b(\mathrm{Inv}_d(y)) \oplus c$

Claim 20

$(\mathrm{G}, \mathrm{E}, \mathrm{D})$ has public-key indistinguishable encryptions for a multiple messages

Proof:

We believe that public-key encryptions schemes are “more complex" than private-key ones

Section 3

Active Adversaries

Active Adversaries

- Chosen plaintext attack (CPA):

  The adversary can ask for encryption and choose the messages to distinguish accordingly

- Chosen ciphertext attack (CCA):

  The adversary can also ask for decryptions of certain messages

- In the public-key settings, the adversary is also given the public key
- We focus on indistinguishability, but each of the above definitions has an equivalent semantic security variant.

CPA Security

Let $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ be an encryption scheme. For a pair of algorithms $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$, $n \in \mathbb{N}$, $z \in \{0,1\}^*$ and $b \in \{0,1\}$, let:

Experiment 21 ($\mathsf{Exp}^{\mathsf{CPA}}_{\mathsf{A},n,z}(b)$)

1. $(e, d) \leftarrow G(1^n)$
2. $(m_0, m_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot)}(1^n, z)$, where $|m_0| = |m_1|$.
3. $c \leftarrow \mathsf{E}_e(m_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot)}(1^n, s, c)$

Definition 22 (private key CPA)

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions in the private-key model under CPA attack, if $\forall$ PPT $\mathsf{A}_1, \mathsf{A}_2$, and poly-bounded $\{z_n\}_{n \in \mathbb{N}}$:

$$|\Pr[\mathsf{Exp}^{\mathsf{CPA}}_{\mathsf{A},n,z_n}(0) = 1] - \Pr[\mathsf{Exp}^{\mathsf{CPA}}_{\mathsf{A},n,z_n}(1) = 1]| = \mathsf{neg}(n)$$

CPA Security, cont.

- public-key variant.
- The scheme from Construction 17 has indistinguishable encryptions in the private-key model under CPA attack (for short, private-key CPA secure)
- The scheme from Construction 19 has indistinguishable encryptions in the public-key model under CPA attack (for short, public-key CPA secure)
- In both cases, definitions are not equivalent (?)

CCA Security

Experiment 23 ($\mathrm{Exp}^{\mathrm{CCA1}}_{\mathsf{A},n,z}(b)$)

1. $(e,d) \leftarrow G(1^n)$
2. $(m_0, m_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot),D_d(\cdot)}(1^n, z)$, where $|m_0| = |m_1|$.
3. $c \leftarrow \mathsf{E}_e(m_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot)}(1^n, s, c)$

Experiment 24 ($\mathrm{Exp}^{\mathrm{CCA2}}_{\mathsf{A},n,z_n}(b)$)

1. $(e,d) \leftarrow G(1^n)$
2. $(m_0, m_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot),D_d(\cdot)}(1^n, z)$, where $|m_0| = |m_1|$.
3. $c \leftarrow \mathsf{E}_e(m_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot),D_d^{\neg c}(\cdot)}(1^n, s, c)$

CCA Security, cont.

Definition 25 (private key CCA1/CCA2)

$(\mathsf{G},\mathsf{E},\mathsf{D})$ has indistinguishable encryptions in the private-key model under $x \in \{\mathsf{CCA1},\mathsf{CCA2}\}$ attack, if $\forall$ PPT $\mathsf{A}_1,\mathsf{A}_2$, and poly-bounded $\{z_n\}_{n\in\mathbb{N}}$:

$$|\Pr[\mathsf{Exp}^{x}_{\mathsf{A},n,z_n}(0)=1]-\Pr[\mathsf{Exp}^{x}_{\mathsf{A},n,z_n}(1)=1]|=\mathsf{neg}(n)$$

- The public key definition is analogous

Private-key CCA2

- Is the scheme from Construction 17 private-key CCA1 secure?
- CCA2 secure?

Let $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ be a private-key CPA scheme, and let $(\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrfy})$ be an existential unforgeable strong MAC.

Construction 26

- $\mathsf{G}'(1^n)$: Output $(e \leftarrow \mathsf{G}_E(1^n), k \leftarrow \mathsf{Gen}_M(1^n))$.[a]
- $\mathsf{E}'_{e,k}(m)$: let $c = \mathsf{E}_e(m)$ and output $(c, t = \mathsf{Mac}_k(c))$
- $\mathsf{D}_{e,k}(c,t)$: if $\mathsf{Vrfy}_k(c,t) = 1$, output $\mathsf{D}_e(c)$. Otherwise, output $\perp$

[a] We assume wlg. that the encryption and decryption keys are the same.

Theorem 27

Construction 26 is a private-key CCA2-secure encryption scheme.

Proof: An attacker on the CCA2-security of $(\mathsf{G}', \mathsf{E}', \mathsf{D}')$ yields an attacker on the CPA security of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$, or the existential unforgettably of $(\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrfy})$.

Public-key CCA1

Let $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ be a public-key CPA scheme and let (P, V) be a $\mathcal{NIZK}$ for $\mathcal{L} = \{(c_0, c_1, pk_0, pk_1) \colon \exists (m, z_0, z_1) \quad \text{s.t.} \quad c_0 = \mathsf{E}_{pk_0}(m, z_0) \wedge c_1 = \mathsf{E}_{pk_1}(m, z_1)\}$

Construction 28 (The Naor-Yung Paradigm)

- $\mathsf{G}'(1^n)$:
  1. For $i \in \{0, 1\}$: set $(sk_i, pk_i) \leftarrow \mathsf{G}(1^n)$.
  2. Let $r \leftarrow \{0, 1\}^{\ell(n)}$, and output $pk' = (pk_0, pk_1, r)$ and $sk' = (pk', sk_0, sk_1)$
- $\mathsf{E}'_{pk'}(m)$:
  1. For $i \in \{0, 1\}$: set $c_i = \mathsf{E}_{pk_i}(m, z_i)$, where z_i is a uniformly chosen string of the right length
  2. $\pi \leftarrow \mathsf{P}((c_0, c_1, pk_0, pk_1), (m, z_0, z_1), r)$
  3. Output (c_0, c_1, π).
- $\mathsf{D}'_{sk'}(c_0, c_1, \pi)$: If $\mathsf{V}((c_0, c_1, pk_0, pk_1), \pi, r) = 1$, return $\mathsf{D}_{sk_0}(c_0)$. Otherwise, return $\perp$.

Public-key CCA1, cont.

- We assume for simplicity that the encryption key output by $\mathsf{G}(1^n)$ is of length at least n. (?)
- ℓ is an arbitrary polynomial, and determines the maximum message length to encrypt using ”security parameter" n.

Is the scheme CCA1 secure?

Theorem 29

Assuming (P, V) is adaptive secure, then Construction 28 is a public-key CCA1 secure encryption scheme.

Proof: Given an attacker A' for the CCA1 security of $(\mathsf{G}', \mathsf{E}', \mathsf{D}')$, we use it to construct an attacker A on the CPA security of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ or the adaptive security of (P, V).

Proving Thm 29

Let $\mathsf{S} = (\mathsf{S}_1, \mathsf{S}_2)$ be the (adaptive) simulator for $(\mathsf{P}, \mathsf{V}, \mathcal{L})$

Algorithm 30 (A)

Input: $(1^n, pk)$

1. Let $j \leftarrow \{0,1\}$, $pk_{1-j} = pk$, $(pk_j, sk_j) \leftarrow \mathsf{G}(1^n)$ and $(r, s) \leftarrow \mathsf{S}_1(1^n)$
2. Emulate $\mathsf{A}'(1^n, pk' = (pk_0, pk_1, r))$:

   On query (c_0, c_1, π) of A' to D':
   If $\mathsf{V}((c_0, c_1, pk_0, pk_1), \pi, r) = 1$, answer $\mathsf{D}_{sk_j}(c_j)$.
   Otherwise, answer $\perp$.
3. Output the pair (m_0, m_1) that A' outputs
4. On challenge c ($= \mathsf{E}_{pk}(m_b)$):
   - Set $c_{1-j} = c$, $c_j = \mathsf{E}_{pk_j}(m_a)$ for $a \leftarrow \{0,1\}$, and $\pi \leftarrow \mathsf{S}_2((c_0, c_1, pk_0, pk_1), r, s)$
   - Send $c' = (c_0, c_1, \pi)$ to A'
5. Output the value that A' does

Proving Thm 29, cont.

Claim 31

Assume A' breaks the CCA1 security of (G', E', D') w.p. $\delta(n)$, then A breaks the CPA security of (G, E, D) w.p. $(\delta(n) - \text{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[A' \text{ “makes" } A(1^n) \text{ decrypt an invalid cipher}] = \text{neg}(n) \tag{2}$$

Assume for simplicity that the above prob is 0.
Hence, in the first the emulation of A' is perfect and leaks no information about j.

Let $A'(1^n, x, y)$ be A''s output in the emulation induced by $A(1^n)$, conditioned on $a = x$ and $b = y$.

1. Since no information about j has leaked, $A'(1^n, 0, 1) \equiv A'(1^n, 1, 0)$
2. The adaptive zero-knowledge of (P, V) yields that $|\Pr[A'(1^n, 1, 1) = 1] - \Pr[A'(1^n, 0, 0) = 1]| \geq \delta(n) - \text{neg}(n)$

Proving Thm 29, cont..

Let $A(x)$ be A's output on challenge $E_{pk}(m_x)$ (and security parameter 1^n).

$$
\begin{aligned}
&|\Pr[A(1) = 1] - \Pr[A(0) = 1]| \\
&= \left|\frac{1}{2}(\Pr[A'(0,1) = 1] + \Pr[A'(1,1) = 1]) - \frac{1}{2}(\Pr[A'(0,0) = 1] + \Pr[A'(1,0) = 1])\right| \\
&\geq \frac{1}{2}\left|\Pr[A'(1,1) = 1] - \Pr[A'(0,0) = 1]\right| - \frac{1}{2}\left|\Pr[A'(1,0) = 1] - \Pr[A'(0,1) = 1]\right| \\
&\geq (\delta(n) - \mathrm{neg}(n))/2 - 0
\end{aligned}
$$

Public-key CCA2

- Is Construction 28 CCA2 secure?
- **Problem:** Soundness might not hold with respect to the simulated CRS, after seeing a proof for an invalid statement
- **Solution:** use simulation sound $\mathcal{NIZK}$